UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,960	09/03/2004	Alexander Shipp	117-516	1450

23117 7590 02/28/2008

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	PAPER NUMBER
2134	
MAIL DATE	DELIVERY MODE
02/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/500,960	SHIPP, ALEXANDER	
	Examiner	Art Unit	
	ANDREW L. NALVEN	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4 and 6-9, 11-12* is/are rejected.

7)☒ Claim(s) *5 and 10* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 July 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-12 are pending.

Response to Arguments

2. Applicant's arguments filed 1/22/2008 have been fully considered but they are not persuasive.

3. Applicant argues on pages 9-12 that Stolfo fails to teach examining the executable attachment and comparing the extracted structural elements to determine whether the executable attachment contains code, data or encoded data that could have created the structural elements extracted earlier. Examiner respectfully disagrees. Stolfo teaches examining the executable attachment and comparing the extracted structural elements to determine whether the executable attachment contains code, data or encoded data that could have created the structural elements extracted earlier (Stolfo, paragraph 0061, data analysis component examines records about attachments to determine if malicious, paragraphs 0019-0020). Stolfo teaches the limitation by teaching that an executable is examined and modeled by looking at the structural elements of the emails to which it is attached (Stolfo, paragraphs 0019-0020). Stolfo's virus detection system looks at structural elements of the emails including destination addresses and the email source address (Stolfo, paragraph 0020). The virus detection system then determines whether an attachment is malicious based a comparison of the

recorded structural elements to a particular attachment (Stolfo, paragraph 0020). The claims as currently presented are anticipated by Stolfo because the claimed “examining" of the executable attachment may be reasonably interpreted to include Stolfo's examination of a particular attachment and the collection of related structural statistics in order to determine if a virus is present. Examiner suggests an amendment to more adequately reflect what Applicant views as his invention by narrowing the “examining” limitation to reflect that an internal comparison of structural elements of an email with structural internal elements of the attachment is completed.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. **Claims 1-4, 6-9, 11, and 12 are rejected under 35 U.S.C. 102(e)** as being anticipated by Stolfo et al US PGPub 2003/0167402.

5. **With regards to claims 1, 11, 12,** Stolfo teaches a method of anti-virus processing an email having an executable attachment comprising the steps, executed

by a machine (Stolfo, paragraph 0045, mail server extracts attachments and analyzes attachments for malicious code), of: a) extracting structural elements from the email (Stolfo, paragraph 0044, mail is logged noting the set of properties for that email); b) examining the executable attachment and comparing the extracted structural elements to determine whether the executable attachment contains code, data or encoded data that could have created the structural elements extracted earlier (Stolfo, paragraph 0061, data analysis component examines records about attachments to determine if malicious, paragraphs 0019-0020); and c) signalling that the attachment is possibly viral or not on the basis of the extent to which the examining step b) finds evidence that the structural elements have been created by that attachment (Stolfo, paragraph 0054, attachment is malicious if birth rate of new emails is too high, paragraph 0046, looks at portions of email that are replicated without change).

6. **With regards to claim 2**, Stolfo teaches the structural elements are categorized and the step c) includes assigning a numeric score for each element which could have been created by that attachment, and signaling that the attachment is possibly viral or not on the basis of an overall score (Stolfo, paragraph 0054, attachment is malicious if birth rate of new emails is too high, paragraph 0051, statistical model relating to attachment behavior, paragraph 0057, notes reference code, sender, receiver, number of recipients).

7. **With regards to claim 3**, Stolfo teaches that the scores are weighted according to category (Stolfo, paragraphs 0059-0061, probabilistic model generates numerical figure from analysis of data records).

8. **With regards to claim 4**, Stolfo teaches signaling step c) takes account of factors including any or all of the following attributes of the email: standard MIME headers; unusual MIME headers; deviations from RFC standards; unusual constructs; number of attachments; type of attachments; encoding method used for attachments; text content of the email; and HTML or XHTML content of the email (Stolfo, paragraph 0057, notes reference code, sender, receiver, number of recipients, paragraph 0054, birth rate of new emails with the attachment).

9. **With regards to claim 6**, Stolfo teaches a system for anti-virus processing an email having an executable attachment comprising the following means, implemented by a machine (Stolfo, paragraph 0045, mail server extracts attachments and analyzes attachments for malicious code): a) means for extracting structural elements from the email (Stolfo, paragraph 0044, mail is logged noting the set of properties for that email); b) means for examining the executable attachments for code, data or encoded data that could have created the structural elements extracted earlier (Stolfo, paragraph 0061, data analysis component examines records about attachments to determine if malicious); and c) means for signaling that the attachment is possibly viral or not on the basis of the extent to which the examining step b) finds evidence that the structural elements have been created by that attachment (Stolfo, paragraph 0054, attachment is malicious if birth rate of new emails is too high, paragraph 0046, looks at portions of email that are replicated without change).

10. **With regards to claim 7**, Stolfo teaches the structural elements are categorized and the means c) includes means for assigning a numeric score for each element which

could have been created by that attachment, and signaling that the attachment is possibly viral or not on the basis of an overall score (Stolfo, paragraph 0054, attachment is malicious if birth rate of new emails is too high, paragraph 0051, statistical model relating to attachment behavior, paragraph 0057, notes reference code, sender, receiver, number of recipients).

11. **With regards to claim 8**, Stolfo teaches the scores are weighted according to category (Stolfo, paragraphs 0059-0061, probabilistic model generates numerical figure from analysis of data records).

12. **With regards to claim 9**, Stolfo teaches the signalling step c) takes account of factors including any or all of the following attributes of the email: standard MIME headers; unusual MIME headers; deviations from RFC standards; unusual constructs; number of attachments; type of attachments; encoding method used for attachments; text content of the email; and HTML or XHTML content of the email (Stolfo, paragraph 0057, notes reference code, sender, receiver, number of recipients, paragraph 0054, birth rate of new emails with the attachment).

Allowable Subject Matter

Claims 5 and 10 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

13. The following is a statement of reasons for the indication of allowable subject matter: The cited prior art, Stolfo and Schultz, teach methods of detecting viruses in emails. However, the cited prior art fails to specifically teach a means for extracting the structural elements as strings and examining the attachments for matches of those strings and signaling the attachment as possibly viral or not on the basis of the extent to which the examining finds occurrences of the strings in the attachment. Thus, the cited prior art fails to anticipate or render obvious the above-cited claims.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Andrew L Nalven/

Examiner, Art Unit 2134

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2132